INFORMATION PAPER

SAIS-IOT-B
29 March 2004

SUBJECT: General Accounting Office Report (GAO-04-467) – Information Security – Technologies to Secure Federal Agencies, March 2004

1. Purpose. To provide a review of the GAO report (GAO-04-467) on cybersecurity technologies that includes a section on authentication technologies and biometrics.

2. Background.

   - GAO was asked by the Chairmen of the House Committee on Government Reform (Representative Tom Davis) and its Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census (Representative Adam Putnam) to identify commercially available, state-of-the-practice cybersecurity technologies that federal agencies can use to defend their computer systems against cyber attacks.

   - The GAO report is a guide that builds on the *Federal IT Security Assessment Framework* that the National Institute of Standards and Technology (NIST) developed for the Federal Chief Information Officer Council.

3. Objectives of the Report.

   - Provide a structured discussion of commercially available, state-of-the-practice cybersecurity technologies that federal agencies can use to secure their computer systems.

   - Identify 18 cybersecurity technologies that can serve as safeguards and countermeasures to protect agencies' information technology (IT) infrastructures.

   - Frame discussion of the specific cybersecurity technologies by the control functionality: access controls, system integrity, cryptography, audit and monitoring, configuration management and assurance.

   - Describe cybersecurity technologies by what they do, how they work, and their reported effectiveness.

4. Key Points.

   - ***Access Control technologies*** focus on boundary protection (firewalls and content management), authentication (biometrics and security tokens), and authorization (user rights and privileges).

Boundary Protection Technologies

- ***Firewall technologies*** include stateful inspection firewalls (network connections that transfer data); application proxy gateway firewalls (intermediary between applications and external servers); dedicated proxy servers (behind firewall platforms); hybrid firewall technologies (combined different types of firewall platforms); network address translation (hide network addresses); host-based firewalls (firewall software components); personal firewalls (secure home/remote PCs); and centrally managed distributed firewalls (centrally controlled/locally enforced).

- When properly configured, all firewalls can protect the network or PC from unauthorized access through the network. However, it is important to consider the strengths and weaknesses of each type of firewall platform.

- ***Content management technologies*** monitor Web and messaging applications to filter inappropriate content, spam, intellectual property breach, noncompliance with an organization's security policies, and banned file types.

- Content filters have significant rates of both erroneously accepting objectionable sites and blocking sites that are not objectionable.

Authentication Technologies

- ***Biometric technologies*** are authentication techniques used to verify identity by measuring and analyzing human characteristics, such as fingerprints, irises, and voices.

- Biometric identification systems are essentially pattern recognition systems that use acquisition devices, such as cameras and scanning devices, to capture images, recordings, or measurements of an individual's characteristics, and use computer hardware and software to extract, encode, store, and compare these characteristics.

- The biometric process is divided into two stages: (1) enrollment and (2) verification or identification.

- Current biometric technologies that are used to protect computer systems from unauthorized access include fingerprint, iris, or voice recognition.

- ***Fingerprint recognition technologies*** illustrated included hardware devices that capture fingerprints in a keyboard (Key Tronic Corporation) or mouse (Siemens PSE TechLab).

- Iris recognition technology illustrated includes a desktop iris recognition system (Matsushita Electric Corporation of America).

- ***Speaker recognition technology*** was not illustrated in the report. Speaker recognition technology uses the distinctive characteristics in the sound of people's voices as a biometric identifier.

- Limitations to the effectiveness of biometric technologies for fingerprints included problems associated with the quality of the template, human physical disabilities, quality of the capture device, and forgeries.

- A vulnerability of speaker authentication is that the voice can be easily recorded and therefore duplicated. However, some speaker verification systems provide safeguards against the use of a recorded voice to trick the system.

- ***Smart token technologies*** are easily portable devices that contain an embedded integrated circuit chip that is capable of both storing and processing data.

- When used to provide a stronger and more convenient means for users to identify and authenticate themselves to computer and networks, a smart token is an example of authentication based on something that a user possesses. However, typical smart token implementations also require a user to provide something he or she knows, such as a password.

- Smart tokens can be classified according to physical characteristics (smart cards), interfaces (smart tokens with an electronic interface for special readers and writers), and protocols (three main methods for authentication, such as static password exchange and time-synchronized and challenge-response based on cryptography).

- If implemented correctly, smart tokens can help to create a secure authentication environment. However smart tokens do not necessarily verify a person's identity; they only confirm that a person has the token. Token theft or loss and algorithm tampering create vulnerabilities as stand-alone systems to protect extremely sensitive data.

- Smart token systems are considered more effective when combined with other methods of authentication, such as biometric identification.

- ***Authorization: User Rights and Privileges technologies*** grant or deny access to a protected resource, whether it is a network, system, individual computer, program, or file. Typically, user rights and privileges are capabilities that are built into an operating system, access control software, and communication protocols.

- Typical technologies include use of algorithms and user-based rules (access control software) and TACACS+ and RADIUS (communication protocols).

- A key component in implementing adequate access controls is ensuring that appropriate user rights and privileges have been assigned. If a user has too many rights or has rights to a few key functions, the organization can be susceptible to fraud.

System Integrity

- ***System integrity technologies*** are used to ensure that a system and its data are not illicitly modified or corrupted by malicious code. ***Anti-virus software*** and ***integrity checkers*** are two types of technologies that help to protect against malicious code attacks.

- Malicious code includes viruses (programs that infect computer files), Trojan horses (computer program that conceals harmful code), and worms (independent computer program that reproduces by copying itself from one system to another).

- Anti-virus software technologies include signature scanners, activity blockers, and heuristic scanners.

- Signature scanners are effective against viruses; activity blockers are more successful against Trojan horses and worms; heuristic scanners are able to detect unknown viruses.

- ***File Integrity Checkers*** are software programs that monitor alterations to files that are considered critical either to the organization or the operations of the computer.

- File integrity checkers perform intrusion detection, administration, policy enforcement, identification of hardware or software failure, and forensic analysis.

- File integrity checkers are effective if the baseline database is not corrupted and must be updated whenever significant changes are made to the system. Also, integrity checkers may generate false alarms when authorized changes are made to monitored files.

Cryptography

- ***Cryptography*** is used to secure transactions by providing ways to ensure data confidentiality (assurance that the information will be protected from unauthorized access), data integrity (assurance that data have not been accidentally or deliberately altered, authentication of the message's originator, electronic certification of data, and nonrepudiation (proof of the integrity and origin of data that can be verified by a third party).

- Cryptographic techniques are two basic types. ***Secret key cryptography*** employs algorithms in which the key that is used to encrypt the original plaintext message can be calculated from the key that is used to decrypt the ciphertext message, and vice versa. ***Public key cryptography*** employs algorithms designed so that the key that is used to encrypt the original plaintext message cannot be calculated from the key that is used to decrypt the ciphertext message.

- Secret key cryptography has significant limitations that can make it impractical as a stand-alone solution for securing electronic transactions, especially among large communities of users who may have no preestablished relationships. Key management may create immense logistical problems and delays.

- Public key cryptography can address many of the limitations of secret key cryptography regarding key management. It is impractical and unrealistic to expect that each user will have previously established relationships with all of the other potential users in order to obtain their public keys. Furthermore, although a sender can provide confidentiality for a message by encrypting it with the recipient's publicly available encryption key using public key algorithms for large messages, this is computationally time-consuming and could make the whole process unreasonably slow.

- Encryption technology is effective only if it is an integral part of an effectively enforced information security policy that includes good key management practices.

- ***Digital signature technologies*** use cryptography to authenticate the sender of a message. Properly implemented digital signatures use public key cryptography to provide authentication, data integrity, and nonrepudiation for a message or transaction. By linking an individual to his or her public key, digital certificates help to provide assurance that digital signatures are used effectively. However, digital certificates are only as secure as the public key infrastructure that they are based on.

- ***Virtual private networks (VPN)*** use cryptography to establish a secure communications link across unprotected networks. VPNs are typically used in intranets and in remote access connections. There are two main VPN technologies. Tunneling protocols encrypt packets at the sending end and decrypt them at the receiving end. SSL protocols connect users to services and applications inside private networks, but they secure only the applications' services or data. SSL is a feature of commonly available commercial Web browsers.

- VPNs are only as secure as the computers that are connected to them. VPNs may be susceptible to man-in-the-middle attacks, message replay attacks, and denial-of-service attacks.

Audit and Monitoring

- ***Audit and monitoring technologies*** can help security administrators to routinely assess computer security, perform investigations during and after an attack, and even recognize an ongoing attack.

- Four types of audit and monitoring technologies are described: intrusion detection systems, intrusion prevention systems, security event correlation tools, and computer forensics.

- An ***intrusion detection system (IDS)*** detects inappropriate, incorrect, or anomalous activity that is aimed at disrupting the confidentiality, availability, or integrity of a protected network and its computer systems. There are three common types of IDS, classified by the source of information they use to detect intrusion: network-based (capture and analyze network packets); host-based (collect information from within an individual computer system and use that

information to detect intrusions); and application-based (analyze the events occurring within a specific software application).

- IDSs cannot instantaneously detect, report, or respond to an attack when there is a heavy network or processing load. Therefore, IDSs are vulnerable to denial-of-service attacks. The effectiveness of an IDS can be somewhat determined by the number of false positives and false negatives that it generates.

- ***Intrusion Prevention Systems (IPS)*** are IDSs with an active response strategy. IPSs (network-based or host-based) not only can detect an intrusive activity, but they also can attempt to stop the activity—ideally before it reaches its targets.

- Network-based IPSs offer in-line monitoring of data streams throughout the network and provide the capability to prevent intrusion attempts. Host-based IPSs allow systems and applications to be configured individually, preventing attacks against the operating system or applications.

- IPSs are susceptible to errors in detecting intrusions. If the detection of incidents is not accurate, then an IPS may block legitimate activities that are incorrectly classified as malicious. Also, IPSs cause bottlenecks in network traffic, reducing throughput across the network.

- ***Security Event Correlation tools*** collect logs, or lists of actions that have occurred, from operating systems, firewalls, applications, IDSs, and other network devices. Then the correlation tools analyze the logs in real time, discern whether an attack has occurred, and respond to a security incident.

- Correlation tools are limited in their ability to interface with numerous security products. They may not be able to collect and correlate logs from certain products. Also, they rely on the sufficiency and accuracy of the logs, and they cannot detect attacks that have bypassed the various security devices. Encryption and authentication to ensure the security and integrity of the data may mitigate this risk.

- ***Computer Forensics tools*** are used to identify, preserve, extract, and document computer-based evidence. They can identify passwords, logons, and other information in files that have been deleted, encrypted, or damaged.

- There are two main categories of computer forensics tools: (1) evidence preservation and collection tools, which prevent the accidental or deliberate modification of computer-related evidence and create a logical or physical copy of the original evidence, and (2) analysis tools, which provide data recovery and discovery functions.

- There are no standards or recognized tests by which to judge the validity of the results produced by these tools. Computer forensics tools must meet the same standards that are applied to all forensic sciences, including formal testable theories, peer-reviewed methodologies and tools, and replicable empirical research. Failing to apply standards may result in contaminating or losing critical evidence.

Configuration Management and Assurance

- ***Configuration management and assurance technologies*** help security administrators to view and change the security settings on their hosts and networks, verify the correctness of the security settings, and maintain operations in a secure fashion under duress.

- Technologies that assist configuration management and assurance include policy enforcement tools, network management tools, continuity of operations tools, scanners for testing and auditing security, and patch management tools.

- ***Policy enforcement tools*** help administrators define and ensure compliance with a set of security rules and configurations, such as a password policy, access to systems and files, and desktop and server configurations.

- Policy enforcement software can provide for centralized monitoring, control, and enforcement. However, the software's effectiveness is largely governed by the security policies of the organization and can be only as good as the policies that the organization defines.

- ***Network management*** is the ability to control and monitor a computer network from a central location. Five key functional areas of network management include fault management (nodes, network, and network operation); configuration management (network configuration); accounting management (network utilization by users or group); performance management (network performance measurement); security management (network resource control).

- Network management systems can be quite expensive, are often complex; require personnel with specialized training; and cannot support network devices that use vendor-specific products.

- ***Continuity-of-operations tools*** provide a complete backup infrastructure to keep the enterprise's data resources online and available at multiple locations in case of an emergency or planned maintenance, such as system or software upgrading.

- Continuity-of-operations tools include ***high-availability systems*** (two or more computers linked to provide continuous access to data through systems redundancy); ***journaling file systems*** (specific information about data to avoid file system errors and corruption); ***load-balancing technology*** (distributes traffic efficiently among network servers so that no individual server is overburdened); and ***redundant array of independent disk (RAID) technology*** (allows two or more hard drives to work in concert for increased fault tolerance and improved performance).

- Continuity-of-operations technologies can help an agency increase the availability of its mission-critical applications.

- ***Scanners*** help to identify a network's or a system's security vulnerabilities with scanning tools (including port scanners), vulnerability scanners, and modem scanners.

- Port-scanning applications have the capability to scan a large number of hosts, but they do not directly identify known vulnerabilities. Vulnerability scanners can identify vulnerabilities and suggest how to fix them, but they may not themselves have the capability to fix all identified vulnerabilities and might not identify newly discovered vulnerabilities.

- ***Patch management tools*** automate the otherwise manual process of acquiring, testing, and applying patches to multiple computer systems.

- While patch management tools can automate patch delivery, it is still necessary to determine whether a particular patch is appropriate to apply. Patches may need to be tested against the organization's specific systems configurations and tools are not consistently accurate. Furthermore, the automated distribution of patches may be a potential security exposure, because patches are a potential entry point into an organization's infrastructure.

5. Implementation Considerations.

The selection and effective implementation of cybersecurity technologies require adequate consideration of a number of key factors, including:

- Implementing technologies through a layered, defense-in-depth strategy;
- Considering the agency's unique IT infrastructure when selecting technologies;
- Utilizing results of independent testing when assessing the technologies' capabilities;
- Training staff on the secure implementation and utilization of these technologies; and ensuring that the technologies are securely configured.
- Ensuring that the technologies are securely configured.

Defense-in-depth entails implementing a series of protective mechanisms such that if one mechanism fails to thwart an attack, another will provide a backup defense.

The selection of multiple technologies can be made in the context of the overall security infrastructure and not aimed solely at specific components of the system or the network.

Instead of relying on vendors' claims regarding the capabilities of their products, agencies can procure technologies that have been independently tested and evaluated, to ensure that the products meet security standards.

Training is an essential component of a security management program. Personnel who are trained to exercise good judgment in following security procedures can successfully mitigate vulnerabilities.

To effectively implement cybersecurity technologies, such technologies must be securely configured. The effectiveness of various technologies, including firewalls and intrusion detection systems, is highly dependent on proper configuration.

6. References.

The GAO report does not cite any references for the Section – Authentication: Biometrics, pp 25-29. A review of the NIST Special Publications cited in the report did not produce reference information that would indicate sources from which the Biometrics Section was developed.

Upon a phone call inquiry, GAO staff provided the source document for the Biometrics Section, GAO-03-174, *Technology Assessment: Using Biometrics for Border Security*, November 2002.